Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 29 (2012) 2721 – 2725

Procedia Engineering

www.elsevier.com/locate/procedia

2012 International Workshop on Information and Electronics Engineering (IWIEE)

Electronic Voting Scheme About ElGamal Blind-signatures Based on XML

F.Song[a*], Z.Cui[a]

[a]*Chengdu Institute of Computer Applications, Chinese Academy of Sciences ChengDu Information Technology of Chinese Academy of Schences Co.LTD, Chengdu, 610041, China*

Abstract

Present an electronic voting algorithm about ElGamal blind-signature based on XML and analyze its security, accounting to the current electronic voting scheme and the ElGamal blind-signature algorithm. The program uses the specification of XML digital signature and the technology of ElGamal blind-signature algorithm and has good security and practical importance.

Keywords: Electronic Voting; digital signature; blind-signature; ElGamal; XML.

1. Introduction

Electronic voting (E-voting) is a way that voters vote through the Internet, and the votes are counted by the vote center. E-voting is based on a variety of cryptographic technologies which is an important application of cryptography, through the computer and the network to complete the entire voting process. Generally speaking, a reliable e-voting scheme should satisfy the following eight requirements:

1. Legitimacy: only legitimate voters have the right to vote.
2. Completeness: The system is able to certificate and count every vote correctly, and prevent tampering with votes, missing legal votes, adding illegal votes, copying legitimate votes, and disclosing information of votes and so on.
3. Anonymity: the content must be kept confidential, in addition to the voters themselves; no one can associate voters with the vote content.
4. Non-repeatability: any legitimate voters cannot vote repeatedly.

* * Corresponding author. Tel.: +86-0311-8799-4277.
E-mail address: asfei1031@gmail.com

doi:10.1016/j.proeng.2012.01.379

5. Impartiality: before the final voting results announced, any institution or individual cannot get the intermediate result of voting.

6. Verifiability: any person or only the voters can verify whether the final voting results are correct statistics of legitimate votes.

7. Robustness: fatal errors cannot occur when the system is attacked by malicious voters or attackers, and the voting system is able to run normally.

8. Feasibility: installation and configuration of the electronic voting system is acceptable in money and time, and voters do not need extra skills and equipment either.

E-voting has a high level of requirements for network and information security, meanwhile the votes' numbers, voters and other important information are needed to be verified, so an electronic voting scheme which combines XML and ElGamal blind-signature is proposed.

2. Overview of existing e-voting solutions

2.1 The Fujioka blind-signature electronic voting scheme

Because of the anonymity of blind-signature, to construct blind votes concealing voter's identity become an important application of blind-signatures in the electronic electoral system. Domestic and foreign scholars have carried out this line of research and have made great achievements. In 1992, Fujioka proposed a blind-signature based on the e-voting scheme [1], the program's algorithm is easy to implement with low network traffic, which has been widely used in the non-governmental sector. This is a representative of the electronic voting program, but in this program there are some short comings in terms of security: such as the lack of voter control, failed to prevent same voter from voting repeatedly or casting the same votes over and over again.

Currently, Fujioka e-voting program has been improved by many papers and programs [2]-[3].however, there are still some problems in security and efficiency to varying degrees.

2.2 Wei chiku scheme

To improve the practicality of Fujioka e-voting, many domestic and foreign scholars have made a lot of researches. Wei_Chiku and others present a more complex and sophisticated e-voting scheme on this basis in 1999 [3]. They use the user signs tag and a voting decision treated with one-way function h to identify votes together, trying to resolve the "votes collision " issue, to facilitate the supervision of voters, in addition to using more than one vote collectors and scrutinizers to oversee the work of collecting votes. Under these two points, they believe that the difference between total number of registered votes and counting is due to voter abstention, which may transfer to the power department and allow voters quit midway. However, it still cannot stop issuers from faking legitimate votes. And its tag and function h both use random numbers and one-way functions, from the randomness of random numbers and the features of one-way functions, we can see that use them to identify the votes, in essence, which cannot guarantee the uniqueness of the votes, and cannot satisfy the requirements of large-scale voting. In addition, the process of votes' verification is too complicated to promote.

3. Schematic design

3.1 Blind-signature scheme based on ElGamal

In the scheme of blind message signature, the signer only signs the blind message m', but the specific content of the real message m cannot be seen, and such signature is characterized by sig(m)=sig(m') or

sig(m) containing partial data of sig(m') . The signer can confirm the signature on m as long as retains the blind-signature on message m'. For example: A want to get B's signature on message m, B's private key is x, y=αx mod p is B' s public key, p is a random large prime numbers, and α is a generator of Zp-1. First, A selects random selected blind factor h∈Zp–1, calculates β = α hmod p ,m' =mh mod(p－1), and sends (β ,m') to B; then B selects a random number k∈Zp－1， calculates γ = β k modp, s=x• γ + m' •k mod (p－1)， and sends (γ ,s) back to A. A gets sig(m) = (γ , s), and verifies the equation αs =γm•yγmodp, the signature is valid if established.

3.2 Basic thoughts

This program is designed based on the XML technology and the ElGamal blind-signature and ensures the authenticity and security of voting.

(1) Blinding the message: blind the message m to m' based on ElGamal signature scheme.

(2) Generating the key: the generation process of key is as follows: select two large prime numbers p and q randomly, compute n = pq and φ = (p-1) (q-1), then select a number e randomly, which satisfy 1 <e <φ and gcd (e, φ) = 1, and calculate the integer x, making 1 <x <φ and ex = 1 (modφ). So the voter B's public key is y = (n, e, ID), its private key is x; the scrutineer Cn's public key is yCn, its private key is xCn; public key for the drawer D is yD, and its private key is xD.

(3) Establishing and encapsulating the signature: establish the signature ased on XML Digital Signature specification, including the establishment of the element <Reference/>, the establishment of the element <SignedInfo/>, and the establishment of the element <Signature/>. For each vote, the message recipient B (the voters) generates sig (m ') based on ElGamal blind-signature scheme, and encapsulated in element <Signature/>, then sends XML document which has already setted up element <Signature /> to the sender A(the vote center).

(4) Signature verification: the verification is divided into two parts, to verify the authenticity of votes and the effectiveness of votes' information respectively. The votes sender A get (γV,sV)/(γ,s) as the signature of message m from B, and use the drawer D and the voter B's public key to verify the effectiveness of its signature respectively.

(5) The scrutineers: multiple scrutineers to ensure that there will be at least one scrutineer at work any time, and every vote will be counted correctly.

4. Implementation of the program

4.1 Preparation phase

a. Voter B applies for voting at the center of A, digital certificates which should contain B's public key as well as A's signature is issued to B from A, after checking B's identity. Voters save the private key by themselves, and the public key is stored in digital certificates which are signed by A.

b. A provides blind treatment to a specific electronic vote: generates random number e, and then calculates blinding votes. Gets β=αhmodp by using B's public key y; Blinds vote m '= memod (p-1); using the drawer D's public key yD, calculate βD = αh modpD.

c. A encapsulates the blinding message mv '/ m' into the XML document, or provides the URI of mv'/ m' ; its XML format is as follows:

<Signature>
<SignedInfo>
<CanonicalizationMethod/>
<SignatureMethod/>

```
<Reference(URI=?)>
  <Transforms/>
  <DigestMethod/>
  <DigestValue/>
  </Reference>
</SignedInfo>
<SignatureValue/>
<KeyInfo/>
<Object/>
</Signature>
```

d. A will send the XML document including mv '/ m' and the URI of mv '/ m' to B.

4.2 Votes distribution and voting stages

a. Voter B establishes the element <Reference/>.

At first, mv '/ m' is converted by B in accordance with <Transforms />, then B calculates the results of the conversion using abstract algorithm according to <DigestMethod />, and stores the result into <DigestValue/>. Finally, B establishes <Reference/>,which including <Transforms/>、<DigestMethod/> and <DigestValue/>.

b. Voter B establishes the element <SignedInfo/>,which including <CanonicalizationMethod/>、<SignatureMethod/> and <Reference/>.

c. Voter B establishes the element <Signature/>.

At first, B standardized the element <SignedInfo/> according to <CanonicalizationMethod/>, B uses its private key x, to calculate ɣ = β kmodp, s=x• ɣ +m’ •kmod(p－1), and then standardizes s. Finally, B operates the element <SignedInfo/> and s according to <SignatureMethod/>, and stores results in <SignatureValue/>. Finally, B operating the element <SignatureValue/> and s according to <SignatureMethod/>, and stores result in <SignatureValue/> .

d.Voter B establishes the element<Signature/> including <CanonicalizationMethod/>、<SignedInfo/> and <SignatureValue/>.

e.Voter B put its own public key y and the vote public key yD into <KeyInfo/>.

f.Voter B passes the XML document with <Signature/> to A.

g.The above steps will be under the supervision of at least one scrutineer.

4.3 Counting stage

a. To confirm the validity of the vote.

b. To confirm whther the vote has been modified.

(1) A converts mv '/ m' in accordance with <Transforms />;

(2) A calculates the result of the conversion using abstract algorithm according to <DigestMethod />, and compares the results with the contents of <DigestValue/>, goes to the next step if they are same, or that the signature is invalid, then refuses to accept because of the modified message.

c. To confirm a signature.

(1)A standardizes the element <SignedInfo/> and s according to <CanonicalizationMethod/>;

(2)A operates the element <SignedInfo/> and s according to <SignatureMethod/> , and compares the results with the contents of <SignatureValue/>, goes to the next step if they are same, or that the signature is invalid, refuses to accept because of the modified message.

(3)A gets B and D's public key y and yD from <KeyInfo/>, uses the drawer D's private key xD, then calculates ɣD＝βDkmodpD, sD＝xD•ɣ+m’•kDmod(pD－1),and then standardizes s.

(4) A calculates αs=γm•yγmodp, and verifies the effectivess of D’s and B’s signature respectively. If they are both valid, the voting result is valid; if any one is invalid, then votes are illegal, and the voting result is invalid.

5. Security Analysis

This program uses multiple methods to ensure reliability and safety, such as XML Digital Signature specification, ElGamal blind-signature scheme and so on. AS blinding the votes information, votes and voters both take signature verification respectively.

Legality. Every voter will be reviewed at the vote center, and only the legitimate voters can vote.

Completeness. Every vote will have a signature of the person issuing the votes to eliminate the possibility of forged votes, and vote center calculates the results of the conversion using abstract algorithm according to <DigestMethod/>, and compares the results with the contents of <DigestValue/>, to eliminate tampering with the content of votes.

Accuracy. Only legitimate voters can vote, illegal voters or person pretending to be his both can be identified. Illegal voters may masquerade as legitimate ones to apply voting. But every legitimate voter will have their own private key, when issuing the votes, voters have signed with the private key. The vote center verify voters with the public key , illegal voters unable to obtain legitimate voter's private key, thus ensuring the correctness of the voting.

No-repeatability. In this program both the drawers and the voters verify the signature of votes. When issuing the votes, the signature of the drawer is bind with the signature of voter, thus ensuring a legitimate voter can only cast one vote.

Impartiality. Each vote is blinded, before the result is published, no one can know what it is, except the voters themselves.

Verifiability. After the voting, the vote center makes (γD, sD) / (γ, s) of all electronic votes open, any voter can check their votes to see whether they are correctly counted according to their own signatures.

Robustness. The drawer’s and voter's private key is unique, before verification of signatures, the result of voting are not included in the final result, so a malicious attack cannot affect the final result.

Feasibility. The program can be realized by an ordinary computer, no additional technology or equipment is needed, and has better feasibility.

6. Conclusion

In this paper, an electronic voting scheme of signature encapsulated in XML security specifications is designed based on the ElGamal blind-signature algorithm. The program uses the XML digital signature specification and the ElGamal blind-signature algorithm and so on, resolving voters’ fraud in the e-voting and the information of votes is tampered in a better way. Moreover, it prevents same voter from voting repeatedly or casting the same votes over and over again.

References

[1] Chaum D.Blind-signature Systems[A]. Proceedings of CRYPTO’83[C].Plenum Press ,1984

[2]Wei-ChiKu，Sheng-DeWang. Asecure and practical electronic voting scheme. Computer Communications,1999,22:279-286.

[3] Canonical XML W3C Recommendation [EB/OL]

http://www.w3.org/TR/2001/REC-xml-c14n-2001-03-15